FEV FEB 0 1 2017

TOP SECRET//SI//CEO
Cerrid # 32826222

BRIEFING NOTE FOR THE MINISTER OF NATIONAL DEFENCE

Response to the CSE Commissioner's *Review of CSE Cyber Defence Metadata Activities*

(For Action)

Summary

- You received a letter from the CSE Commissioner, dated 5 December 2016, providing the results of his *Review of CSE Cyber Defence Metadata Activities*.
- This is the third report produced from the CSE Commissioner's broad review of CSE's use of metadata that began in 2013. This report presents the CSE Commissioner's findings on the portion of the review covering metadata activities in an information technology (IT) security context.
-
-

Background

- You received a letter from the CSE Commissioner, dated 5 December 2016, providing the results of his *Review of CSE Cyber Defence Metadata Activities*.
- This is the third report produced from the CSE Commissioner's broad review of CSE's use of metadata that began in 2013. This report presents the CSE Commissioner's findings on the portion of the review covering metadata activities in an information technology (IT) security context.

Considerations

Next Steps

- Attached is a proposed package for your consideration and response to the CSE Commissioner.

Greta Bossenmaier
Chief

Communications Security
Establishment Commissioner

The Honourable Jean - Pierre Plouffe, C.D.

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Jean - Pierre Plouffe, C.D.

TOP SECRET//SI//CEO

Our file # 2200–101

December 5, 2016

The Honourable Harjit S. Sajjan, PC, OMM, MSM, CD, MP
Minister of National Defence
101 Colonel By Drive
Ottawa, ON K1A 0K2

Subject: Review of CSE Cyber Defence Metadata Activities

Dear Minister:

The purpose of this letter is to provide you with the results of a review of Communications Security Establishment (CSE) cyber defence metadata activities. I examined CSE use of metadata in an information technology (IT) security context to determine whether it complies with the law and does not direct its cyber defence activities at Canadians or any person in Canada and that it effectively applies satisfactory measures to protect Canadians' privacy. This review is the third and last in a series of recent investigations focused on metadata; the first two parts — submitted in 2015 and March 2016 — addressed foreign signals intelligence metadata activities.

The review was conducted under the Commissioner's general authority set out in paragraph 273.63(2)(*a*) of the *National Defence Act* (NDA) and the authority set out in subsection 273.65(8) of the NDA to determine whether activities carried out under a ministerial authorization (MA) are authorized by the Minister of National Defence. The review was led by a computer engineer and IT security expert contractor with 30 years' experience in the public and private sector, which provided the office with a new perspective on the activities. He examined CSE operational policy and procedures, received technical briefings and demonstrations, and conducted interviews.

CSE conducts cyber defence metadata activities under the authority of paragraph 273.64(1)(*b*) of the NDA and cyber defence MAs. The 2011 ministerial directive on metadata defines metadata as "information associated with a telecommunication to identify, describe, manage or route that telecommunication or any part of it as well as the means by which it was transmitted, but excludes any information or part of information which could reveal the purport of a telecommunication, or the whole or any part of its content." CSE may acquire cyber defence metadata from its own sources, from domestic and international partners, and from owners of computer systems of importance to the Government of Canada (GC).

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
T: 613-992-3044 F: 613-992-4096

Metadata remains essential to CSE's cyber defence mandate, for example, to identify and mitigate sophisticated foreign malicious cyber threats to help protect computer systems of importance to the GC. Past reviews on cyber defence activities conducted under MAs (recently, reports # 2200–104 in 2016 and # 2200–84 in 2015) and not conducted under MAs (report # 2200–69 in 2013) contain detailed background information, including on CSE acquisition and use of metadata for cyber defence activities. The reports and the office's working file also contain specific information on the systems, databases and tools used by CSE to, for example, analyze and retain metadata for cyber defence activities. I will not repeat background information in this letter; however, the following general points are worth noting.

CSE cyber threat detection capabilities copy and store a sub-set of GC client network data — including metadata — to identify and permit ongoing analysis of anomalous and sophisticated foreign malicious cyber events. CSE acquires only a small proportion of the data passing through its cyber defence sensors. CSE extracts metadata from the data acquired and uses it, for example, to contextualize the threat and malware and to develop mitigation advice for the client and other GC institutions.

CSE does not collect unselected (bulk) metadata under part (b) of its mandate (the 2015 review report addressed CSE collection of unselected metadata for the purpose of foreign intelligence under part (a) of its mandate); cyber defence activities acquire from GC networks both content and metadata relating to cyber events.

It is to be expected that CSE cyber defence activities may involve metadata relating to Canadians because the activities involve data from Canadian networks located in Canada — acquired either by CSE under an MA, or by system owners and GC institutions under *Criminal Code* and *Financial Administration Act* authorities and subsequently disclosed to CSE.

CSE cyber defence activities generally acquire communications containing nothing more than malicious code or an element of "social engineering" sent to a computer system in order to deceive the recipient and compromise the system.

Even so, CSE treats cyber defence metadata that could identify a communicant or the communication — for example, the "from" and "to" fields of an e-mail, or an Internet Protocol address linked to the communication — like a private communication (PC) and applies the same privacy protection measures to that metadata as it would to a PC.

s.26

Before this letter was finalized, CSE officials had an opportunity to review it for factual accuracy and to comment on the findings.

If you have any questions or comments, I will be pleased to discuss them with you at your convenience.

Yours sincerely,

Jean-Pierre Plouffe

cc: Ms. Greta Bossenmaier, Chief, CSE

Minister
of National Defence

Ministre
de la Défense nationale

Ottawa, Canada K1A 0K2

SECRET
CERRID # 32825877

FEV
FEB 21 2017

The Honourable Jean-Pierre Plouffe
Communications Security Establishment Commissioner
90 Sparks Street, Suite 730
P.O. Box 1984, Station B
Ottawa, Ontario, K1P 5B4

Dear Commissioner Plouffe:

I am writing to respond to your report dated 5 December 2016, entitled *Review of CSE Cyber Defence Metadata Activities.*

I read with interest your findings concerning CSE's metadata activities in an information technology (IT) security context, which marks the completion of your Office's three-part review of CSE's activities involving metadata that began in 2013.

Thank you for your report.

Sincerely,

The Hon. Harjit S. Sajjan, PC, OMM, MSM, CD, MP

cc: Greta Bossenmaier, Chief, CSE

Canada